与えられた number knot を持つ代数体のメタアーベル拡大について (代数的整数論とフェルマーの問題)

AUTHOR(S):

藤田, 司

CITATION:

藤田, 司. 与えられた number knot を持つ代数体のメタアーベル拡大について(代数的整数論とフェルマーの問題). 数理解析研究所講究録 1996, 971: 40-49

ISSUE DATE:

1996-10

URL:

http://hdl.handle.net/2433/60700

数理解析研究所講究録
971巻 1996年 40-49

与えられたnumber knotを持つ代数体のメタアーベル拡大について

東大 数理 藤田 司

K/k を有限次代数体の有限次拡大とするとき、次式によって K/k のnumber knot $\nu(K/k)$ が定義される。

$\nu(K/k)$ = (local norms)/(global norms) = $(\bigcap N_{K/k} J_K)/N_{K/k} K^\lambda$

(J_K は K のidele group, $N_{K/k}$ はnorm map)

定義により、$\nu(K/k)=0$ ということは、K/k にHasse norm principleが成り立つことを意味する。また $\nu(K/k)$ は有限群であり、特に K/k がGalois拡大の場合には次のTateの定理によりその群が群論的に計算される。

定理[6] K/k: Galois, $G=\mathrm{Gal}(K/k)$ とすると、$\nu(K/k)$ は $\mathrm{Coker}(\bigoplus H_2(G^v,\mathbb{Z}) \xrightarrow{\bigoplus \mathrm{cor}_v} H_2(G,\mathbb{Z}))$ とcanonicalに同型である。ここで $\bigoplus$ は次の全ての素点 v にわたる直和、G^v は v 上にある K のある素点の分解群、corはcorestriction map

この定理により、次の"逆問題" $P(k,G,K)$ が考えられる。

$\mathbb{P}(k, G, K)$: 有限次代数体 k, 有限群 G, $H_2(G, \mathbb{Z})$ の部分群 K が与えられたとする。このとき Galois 拡大 K/k 及び同型 $\Psi: \mathrm{Gal}(K/k) \to G$ で次の可換図式を induce するものが存在するか?

$$\begin{array}{ccc} H_2(\mathrm{Gal}(K/k), \mathbb{Z}) & \xrightarrow[\Psi_*]{\cong} & H_2(G, \mathbb{Z}) \\ \downarrow & & \downarrow \\ J(K/k) & \xrightarrow{\cong} & H_2(G, \mathbb{Z})/K \end{array}$$

もし $H_2(G, \mathbb{Z}) = 0$ なら自動的に $K = 0$ となるので、$\mathbb{P}(k, G, K)$ は通常の Galois 逆問題となる。従って特に G が可解で $H_2(G, \mathbb{Z}) = 0$ を満たすときには $\mathbb{P}(k, G, K)$ は任意の有限次代数体 k に対して成立する。G が可換群のときには、$\mathbb{P}(k, G, K)$ が成り立つためには K が $H_2(G, \mathbb{Z})$ の "typical subgroup" であることが必要十分であることが知られている ([2], [5])

そこで、今回は G が簡単な非可換群のときに上の問題を考察してみた。考えてみたのは次の2通りの場合である。

(1) $G = D_n = \langle a, b \mid a^n = b^2 = 1, bab = a^{-1} \rangle$ dihedral のとき

(2) G が位数 p^3 の非可換群のとき (p: 素数)

結果を先に述べる。

結論 G が上の (1) (2) いずれの場合でも、任意の k, 任意の部分群 $K \subset H_2(G, \mathbb{Z})$ に対し $\mathbb{P}(k, G, K)$ は真となる。

以下この証明の概略を示す。

1. G が dihedral group の場合

$G = D_n = \langle a, b \mid a^n = b^2 = 1,\ bab = a^{-1} \rangle$ とする。

定理([1]) $H_2(D_n, \mathbb{Z}) = \begin{cases} 0 & (n \text{ が奇数のとき}) \\ \mathbb{Z}/2\mathbb{Z} & (n \text{ が偶数のとき}) \end{cases}$

n が奇数のときは $H_2(G, \mathbb{Z}) = 0$ であり、さらに G は可解なので、Tunnell で述べたように $\mathbb{P}(k, G, K)$ は真である。

そこで以下 n は偶数として考察する。その場合 $H_2(G, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ なので、$v(L/k) = 0$, $v(L/k) = \mathbb{Z}/2\mathbb{Z}$ の二つの場合に対応する D_n 拡大 L/k を構成することが問題となる。

定理1. n: 偶数, L/k: 有限次代数体 k の二次拡大とする。このとき、

(a) n 次巡回拡大 K/k で、$\mathrm{Gal}(K/k) = D_n$, $v(L/k) = \mathbb{Z}/2\mathbb{Z}$ となるものが存在する

(b) n 次巡回拡大 K/k で、$\mathrm{Gal}(K/k) = D_n$, $v(L/k) = 0$ となるものが存在する

この定理により G が dihedral の場合 $\mathbb{P}(k, G, K)$ が真であることが分かる。そこでこの章の残りでこれを証明していく。

証明で主に用いるのは次の補題である。

補題1([1]) n: 偶数, $G=\mathrm{Gal}(K/k)\cong D_n$ とするとき、$L(K/k)\cong \mathbb{Z}/2\mathbb{Z}$ となるための必要十分条件は、全ての奇素点 v に対して G_v^0 の 2-Sylow 群が cyclic になることである。

こうして $L(K/k)$ についての条件が分解群に関する条件に変換されたので、分解群がそのような条件を満たす D_n 拡大 K/k を以下構成していく。まず補題を二つ準備しておく。

補題2 L/k: 二次拡大, K/L: 巡回 cyclic とする。このとき、

K/k が D_n 拡大 $\Longleftrightarrow$ $C_k \subset N_{L/k} C_L$ ($C_k = J_k/k^\times$ idele class group)

補題3 K/k, K'/k がともに Galois で $k \subset K' \subset K$ となっているとき準同型 $L(K/k) \to L(K'/k)$ が自然に定義される。さらに K/K' が cyclic で $(K:K')$ と $(K':k)$ が互いに素ならば、この準同型は同型となる。

定理1.(a)の証明の方針

$G=D_n$ の奇数位数の部分群で最大のものを H としたとき、任意の G/H 拡大 K/k はある G 拡大 $\tilde{K}/k$ に埋め込まれる([4])。従って、補題3により n は二のべきと仮定してよい。

$S_1 = \mathrm{Ram}_L(\mathcal{L}_K) \overset{\text{def}}{=}$ ($\mathcal{L}_K$ で分岐するような素点全体) とおき、finite subset $S_2 \subset \mathrm{Spl}_L(\mathcal{L}_K) \overset{\text{def}}{=}$ ($\mathcal{L}_K$ で完全分解するような素点全体) をとり S_2 は $\mathrm{Gal}(\mathcal{L}_K)$-集合、(ii) $\forall w \in S_2$, $n \mid (N_w - 1)$, の2条件をみたすようにとる。(S_2 の位数はいくらでも大きくできる.)

この S_1, S_2 に対し次の3条件を満たすアーベル拡大 F/L の中で最大のものをとる。
- $C_K \subset N_{F/L} C_F$
- $\mathrm{Ram}_L(F/L) \subset S_2 \subset \mathrm{Spl}_L(\mathcal{L}_K)$
- $S_1 \subset \mathrm{Spl}_L(F/L)$

もし F/L が n次cyclicな部分拡大 K/L を持てば、補題2より $K/\mathcal{L}_K$ は n次拡大であり、また $K/\mathcal{L}_K$ における素点の分解群は上の条件より全てcyclicとなるので、補題1より $L(K/\mathcal{L}_K) \cong \mathbb{Z}/n\mathbb{Z}$。

よって、S_2 をうまくとれば $\mathrm{Gal}(F/L)$ が n次cyclicな商群を持つことを示せばよい。

$A = U_L / U_L^n \left(\prod_{w \in S_2} U_w^1 \times \prod_{w \notin S_2} U_w \right)$ とおく。($U_L = \ker(\mathfrak{J}_L \to I_L)$, U_w: L_w の units, U_w^1: L_w の principal units)

類体論により $\mathrm{Gal}(F/L)$ を $\mathfrak{J}_L$ の quotient として表わすことにより自然な準同型 $\varphi : A \to \mathrm{Gal}(F/L)$ を得る。$\ker(\varphi)$, $\mathrm{Coker}(\varphi)$ を計算すると、これは有限群であり、$|S_2|$ の大きさに depend しない定数により位数が上から抑えられる。一方 A は $(\mathbb{Z}/n\mathbb{Z})^{\frac{1}{2}|S_2|}$ と同型な群を部分群に持つ有限群なので、S_2 の大きさを十分大きくとると、その時 $\mathrm{Gal}(F/L)$ は n次cyclicな商群を持つ。□

定理1.(a)の証明の方針

ここでもnは2のべとしてよい。n=2の場合は容易なので、n≠1をして証明する。

定理1(a)で構成したD_n拡大をK/kとする。一方、ℓ/kで分岐も分解もしない素点νをとり、νが分岐するような次の2次拡大E/kをとる。G_kをkの絶対Galois群として、拡大K/k, E/kに対応する準同型をφ: G_k → D_n, χ: G_k → Z/2Zとする。φ(G_L)の位数2の部分群をIm(χ)と同一視することにより、χ̃: G_k → D_nがχからinduceされる。φ'(g) = φ(g)χ̃(g) (g∈G_k)によりφ': G_k → D_nを定義する。φ'は全射であることが示されるので、これからD_n拡大K'/kが得られる。K'/Lは巡回cyclicであり、またこのK'/kにおける分解群はnon-cyclicなので、補題1により、D_n拡大K'/kは定理1(a)の条件を満たしている。 □

2. Gが位数p³の非可換群の場合

この場合、p=2ならGは$Q_8 = \langle a,b \mid a^2=b^2, b^{-1}ab=a^{-1}\rangle$または$D_4$のいずれか、pが奇素数ならGは$E_1 = \langle a,b \mid a^{p^2}=b^p=1, b^{-1}ab=a^{1+p}\rangle$または$E_2 = \langle a,b,c \mid a^p=b^p=c^p=[a,c]=[b,c]=1, c=[a,b]\rangle$のいずれかである。これらの群の$H_2(G,\mathbb{Z})$は次のようになることが知ら

れている。

定理　$H_2(Q_8, \mathbb{Z}) = 0$,　$H_2(D_4, \mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$　　$(p=2)$

$H_2(E_1, \mathbb{Z}) = 0$,　$H_2(E_2, \mathbb{Z}) = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$　$(p \neq 2)$

Q_8もE_1も可解なので、Intro.で述べたように$P(k, Q_8, K)$及び$P(k, E_1, K)$は常に真である。また$G = D_4$の場合は前章で扱ったので、ここでは$G = E_2$として考察していく。

$G = E_2$として計算すると次の補題が得られる。

補題4　K/k：Galois拡大，$G = Gal(K/k) \cong E_2$とする。

(i) $G^{\nu} = G$となる素点νがあれば$\mathcal{U}(K/k) = 0$

(ii) 任意の素点νに対しG^{ν}がcyclicなら$\mathcal{U}(K/k) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

(iii) $G^{\nu_1} \neq G^{\nu_2}$, $|G^{\nu_1}| = |G^{\nu_2}| = p$となる$\nu_1, \nu_2$が存在し，かつ

$G^{\nu} = G$となるものがなければ$\mathcal{U}(K/k) = 0$

(iv) 以上の(i)～(iii)のいずれでもなければ$\mathcal{U}(K/k) \cong \mathbb{Z}/p\mathbb{Z}$

次の定理により、補題4の(ii)(iii)(iv)それぞれの条件に対してE_2拡大K/kが存在するので、$P(k, E_2, K)$は真となる。(χ_1, χ_2がともに位数pで$\varphi_1 : Gal(K/k) \xrightarrow{\sim} E_2$が$P(k, E_2, \chi_1)$の解とすると、この$K/k$及びある$\varphi_2 : Gal(K/k) \xrightarrow{\sim} E_2$が$P(k, E_2, \chi_2)$の解となる。)

定理2. 素数の組 p_1, p_2 で次の条件を満たすものが無数に存在する： $p_1 \in (\mathbb{Z}/p_2\mathbb{Z})^{\times p}$, $p_2 \in (\mathbb{Z}/p_1\mathbb{Z})^{\times p}$, $p_i \equiv 1 \pmod{p}$, $p_i \in Spl_{\mathbb{Q}}(F_i/\mathbb{Q})$ $(i=1,2)$

$F_i/\mathbb{Q}$ $(i=1,2)$ を conductor p_i の p 次巡回拡大として $L = F_1F_2$ とおく。すると2次拡大 $k_0/\mathbb{Q}$ で $\mathbb{Q} \subset L \subset k_0$, $Ram_L(k_0/L) \subset Spl_L(k_0/\mathbb{Q})$ を満たすものが存在する。さらにこの拡大 $k_0/\mathbb{Q}$ として次に挙げる条件 (a) (resp. (b), (c)) を満たすものをとることが出来る。

(a) p_1, p_2 の分解群はともに cyclic

(b) p_1, p_2 の分解群はともに non-cyclic

(c) p_1 の分解群は cyclic で、p_2 の分解群は non-cyclic

ここで構成した拡大 $k_0/\mathbb{Q}$ が条件 (a) (resp. (b), (c)) を満たせば、2次拡大 Fk_0/k は補題4の (ii) (resp. (iii), (iv)) を満たす。」

定理2の証明の方針

p_1, p_2 の存在は Chebotarev's density theorem による。この p_1, p_2 に対して上のように $k_0/\mathbb{Q}$ をとると、$k_0/\mathbb{Q}$ は次の条件を満たす2次拡大 $k_0/\mathbb{Q}$ に延長される。(cf. [4])

- $Gal(k_0/L) = Z(Gal(k_0/\mathbb{Q})) := (\text{center of } Gal(k_0/\mathbb{Q}))$
- $k_0/\mathbb{Q}$ で分岐する素数は高々3個で、それらの分解群は全て位数 p.

明らかにこの拡大 $k_0/\mathbb{Q}$ は条件 (a) を満たしている。

今構成した、条件(a)を満たす拡大 $K_0/\mathbb{Q}$ により全射準同型 $\phi: G_{\mathbb{Q}} \twoheadrightarrow E_2$ が定まる。($\phi(G_L) = Z(E_2)$ が成立している)

次に $q \in Spl_{\mathbb{Q}}(L(\zeta_p)/\mathbb{Q})$ として $F_q/\mathbb{Q}$ を conductor q の p 次巡回拡大とする。この拡大 $F_q/\mathbb{Q}$ により $\chi_q: G_{\mathbb{Q}} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ が定まり、$\mathbb{Z}/p\mathbb{Z}$ を $Z(E_2)$ と同一視することにより $\widetilde{\chi_q}: G_{\mathbb{Q}} \to E_2$ が得られる。

$\phi_q(\sigma) = \phi(\sigma)\widetilde{\chi_q}(\sigma)$ $(\sigma \in G_{\mathbb{Q}})$ により $\phi_q: G_{\mathbb{Q}} \to E_2$ を定義する。この ϕ_q は全射であることが示され、これから E_2 拡大 $K_q/\mathbb{Q}$ が定まる。

素数 q が次の条件(B)を満たせば $K_0 = K_q$ は定理2の条件(ii)を満たし、q が条件(C)を満たせば $K_0 = K_q$ は定理2の条件(i)を満たす:

(B) $q \in Spl_{\mathbb{Q}}(L(\zeta_p)/\mathbb{Q})$, $p_1 \neq (\mathbb{Z}/q\mathbb{Z})^{\times p}$, $p_2 \neq (\mathbb{Z}/q\mathbb{Z})^{\times p}$

(C) $q \in Spl_{\mathbb{Q}}(L(\zeta_p)/\mathbb{Q})$, $p_1 \in (\mathbb{Z}/q\mathbb{Z})^{\times p}$, $p_2 \neq (\mathbb{Z}/q\mathbb{Z})^{\times p}$

この条件(B), (C)を満たす素数 q が無数に存在することは Čebotarev's density theorem によって示される。 □

remark

- 補題4の中に対応する K/k が一般の k に対して存在するかは分かりませんでした。($G^{\nu} = E_2$ となるのは p 上の素点に限られてしまうので、上の手法は使えない)
- 定理1, 2により $P(k, G, K)$ が真であるだけでなく、その解が無数に存在することが分かります。

参考文献

[1]. F. Gerth, The Hasse norm principle in metacyclic extensions of number fields, J. London Math. Soc. (2) 16 (1977) pp 203-208

[2] W. Jehne, On knots in algebraic number theory, J. reine angew Math 311 (1979) pp 215-254

[3] G. Karpilovsky, The Schur Multiplier, Oxford University Press, New York, 1987

[4] J.P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, Boston, 1992

[5] H-D. Steckel, Abelische Erweiterungen mit vorgegebenem Zahlkörper, J. reine angew. Math 330 (1982) pp 93-99

[6] J. Tate, Global class field theory in Algebraic Number Theory (edited by Cassels-Fröhlich). London (1967) pp 162-203